Quantum-Search Algorithms, Quntum Codes and All That...

Presented by
Lajos Hanzo

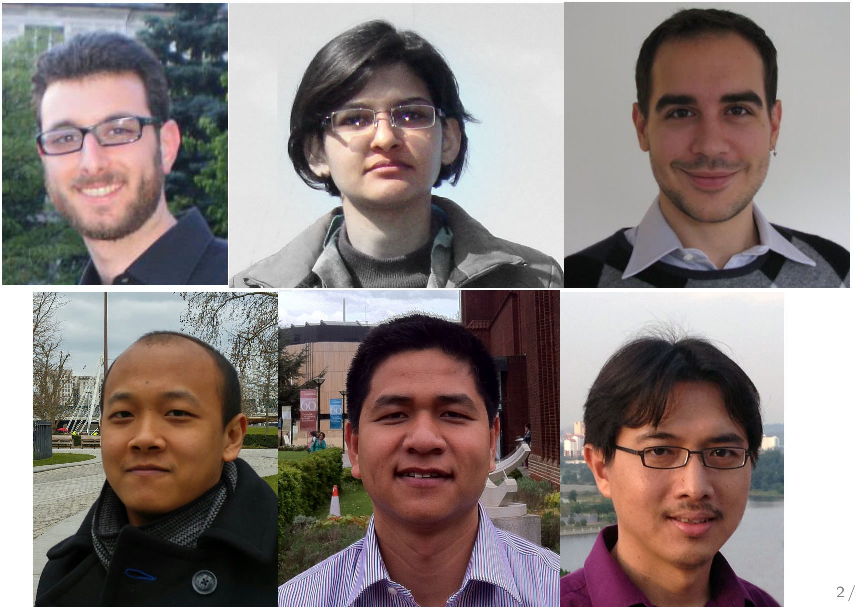
With Dimitrios Alanis, Zunaira Babar, Panagiotis Botsinis, Daryus Chandra, Hung Nguyen, Soon Xin Ng

Southampton Wireless
School of Electronic and Computer Science
University of Southampton
SO17 1BJ, UK
http://www-mobile.ecs.soton.ac.uk

lh@ecs.soton.ac.uk

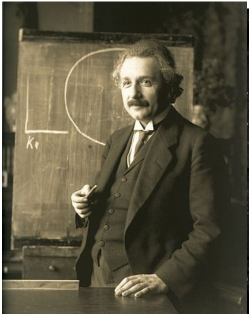
December 21, 2017

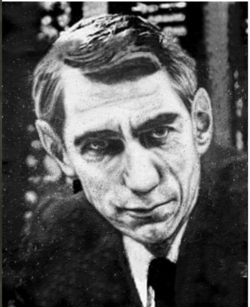
The Dream-Team



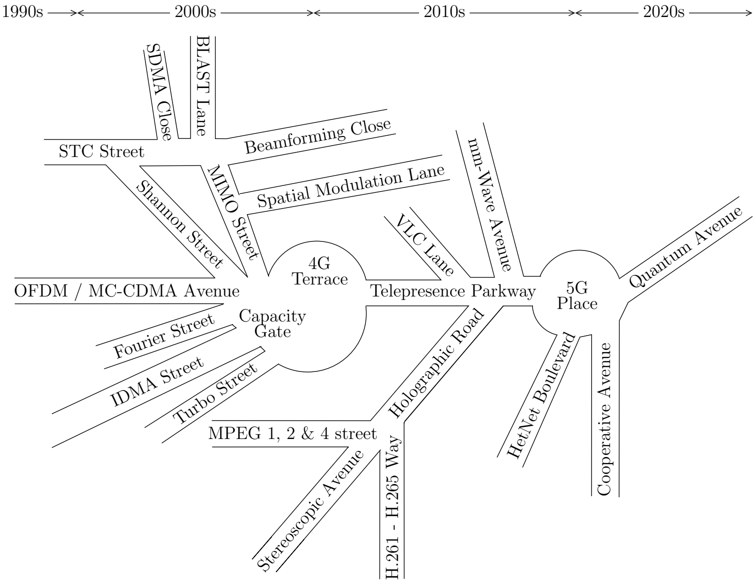
Historic Preamble...

The Founders of our Field





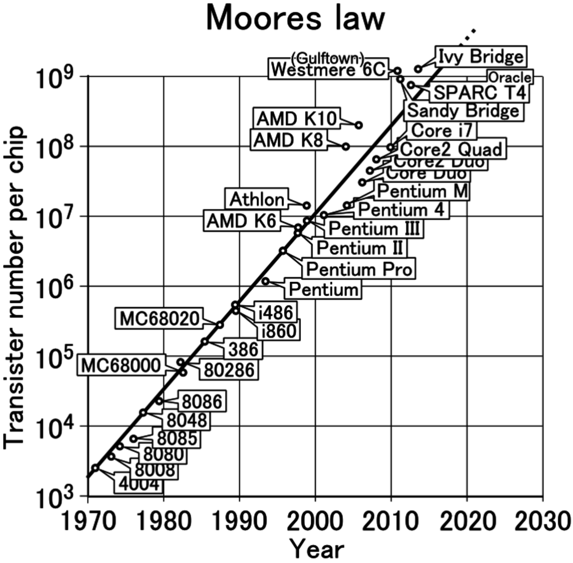
A Stroll with Shannon to Next-Generation Plaza...



Overview

- **History & Introduction to Quantum Computing**
- **EXAMPLE 1 - Quantum Codes for Depolarizing Channels**
- **EXAMPLE 2 - Quantum-Search Assisted Classic Solutions**
- **The Future?**

Moore's Law...

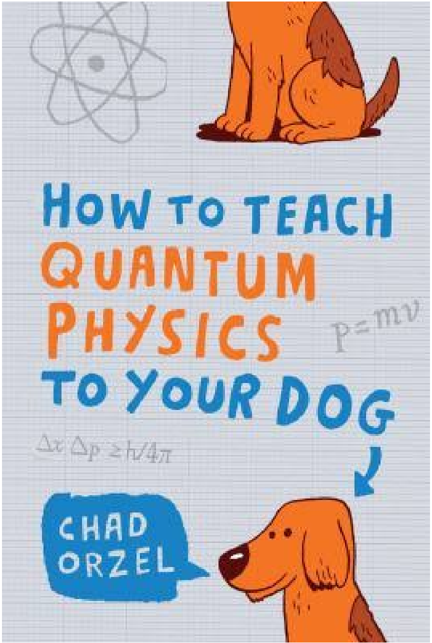


Source: The Conversation

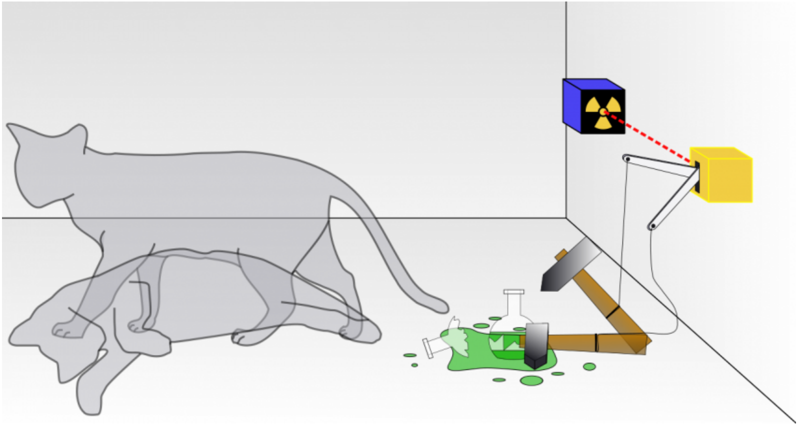
http://theconversation.com/uk/technology

Introduction to Quantum Computing

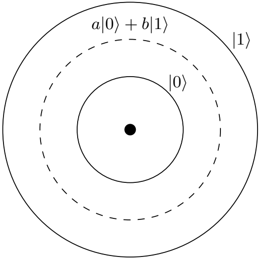
The Quantum-Wireless Saga...



Superposition

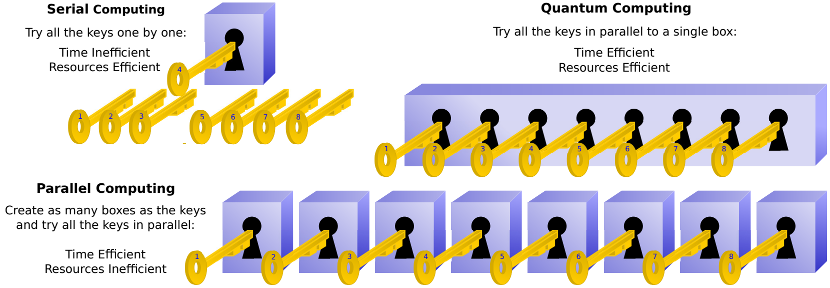


Superposition



An atom with one electron orbiting around the nucleus having two legitimate energy levels (solid orbits). Quantum mechanics allow the electron to be in an arbitrary superposition of these two energy levels (dashed orbit), but when it is observed it may only be found in one of the two legitimate orbits.

The Quantum-Wireless Saga...



Serial Computing

Try all the keys one by one:

Time Inefficient
Resources Efficient

Quantum Computing

Try all the keys in parallel to a single box:

Time Efficient
Resources Efficient

Parallel Computing

Create as many boxes as the keys
and try all the keys in parallel:

Time Efficient
Resources Inefficient

- **[Hanzo et al.]** Wireless Myths, Realities and Futures, Proc. of the IEEE, 13th of May 2012, Centennial Issue, Xplore Open Access
- **[Botsinis, Ng & Hanzo]**: Quantum Search Algorithms, Quantum Wireless and a Low-Complexity Maximum Likelihood Iterative Quantum Multi-User Detector Design, IEEE Access, May 2013, Xplore Open Access

How to Teach Quantum Computing to Your Dog...©Orzel

- Spinning Coin in a Black Box:
  - 50% “Heads” AND 50% “Tails”.
    Both at the same time!
  - Observation (by opening the box): “Heads” OR “Tails”.
  - Idea: Keep the coin spinning and manipulate it without opening the box.

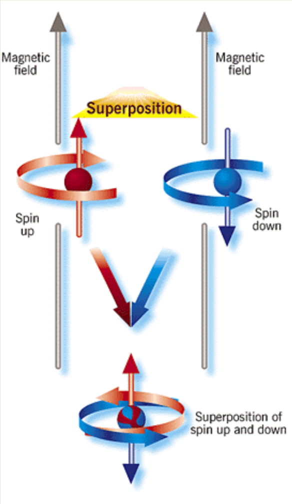
- Coins in computing:
  - Classic bit: 0 or 1.
  - Quantum bit (Qubit): 0 or 1, or any combination of them.
- Ket notation: $|q\rangle = a|\text{HEADS}\rangle + b|\text{TAILS}\rangle = a|0\rangle + b|1\rangle$, where $|a|^2 + |b|^2 = 1$ and $a, b \in \mathbb{C}$.

  Provides any possible superposition of 0 and 1!
- Observation:
  - $|a|^2$ probability to observe $|0\rangle$
  - $|b|^2$ probability to observe $|1\rangle$

  The qubit’s state becomes the observed one with probability 1.
- 2 qubits: $|q\rangle = 0.5|00\rangle + 0.5|01\rangle + 0.5|10\rangle + 0.5|11\rangle$

Motivation: Quantum Parallelism

Qubit: $\alpha|0\rangle + \beta|1\rangle$



http://abyss.uoregon.edu/ js/cosmo/lectures/lec08.html

Quantum Measurement

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle &\xrightarrow{|\alpha|^2} |0\rangle \\ &\xrightarrow{|\beta|^2} |1\rangle \end{aligned}$$

The Future?

So, what are we to do Dr Einstein...?

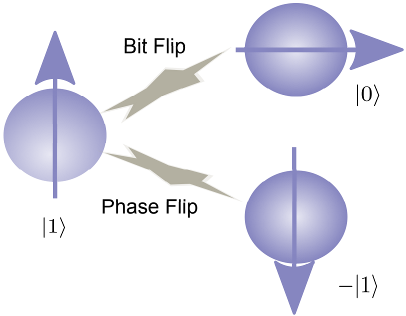
The Future?

Just make sure you eliminate quantum-flips...

But how Dr Einstein...?

Motivation: Eliminate Quantum Decoherence

The Benefits of Quantum Codes

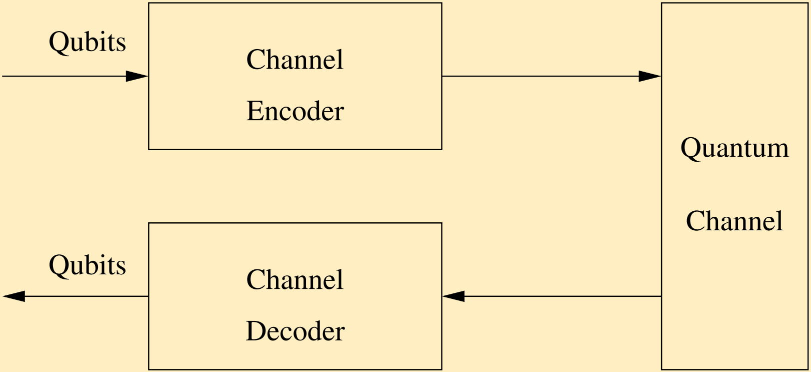


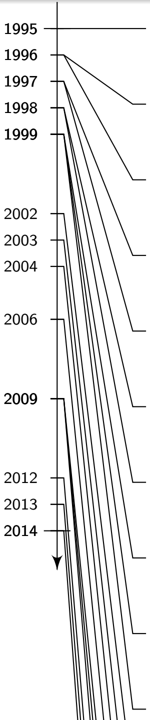
Quantum decoherence/noise characterized by bit and phase flips.

Quantum Error Correction Codes (QECCs) are vital for reliable quantum computing and communication systems.

Research Objective

Design efficient error correction codes for reliable quantum systems by exploiting the underlying quantum-to-classical isomorphism.





Shor Code, *non dual-containing CSS* [1]. The pioneering work on QECC, which introduced 9-qubit code

Steane Code, *dual-containing CSS* [2]. A 7-qubit code was proposed to protect a single qubit.

Laflamme Code, *non-CSS* [3]. The "perfect" 5-qubit code protecting a single qubit.

The general formulation of QSCs was proposed, which is the general concept of syndrome-based QECC

Toric Codes, *non dual-containing CSS* [5, 6]. The first class of QSC based on topological order, where t and have a growing minimum distance with codeword length.

Surface Codes, *non dual-containing CSS* [7]. They constitute an extension of toric codes, where the qu

Quantum GF(4) Codes, *non-CSS* [8]. A wide range of non-CSS QSCs was derived from classical error c

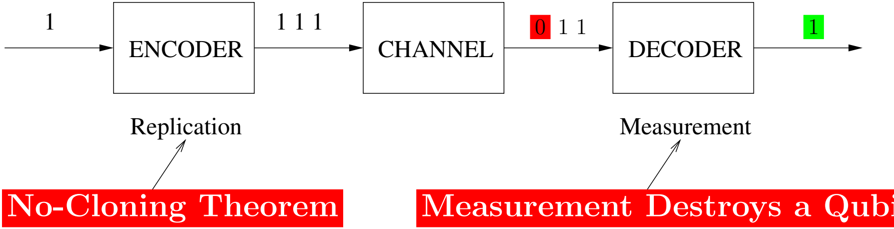
Quantum BCH Codes, *dual-containing CSS* [9]. Inspired by classical BCH codes.

Quantum Reed-Solomon Codes, *dual-containing CSS* [10]. Inspired by classical Reed-Solomon codes.

Quantum Reed-Muller Codes [11], *non-CSS*. Inspired by classical Reed-Muller codes.

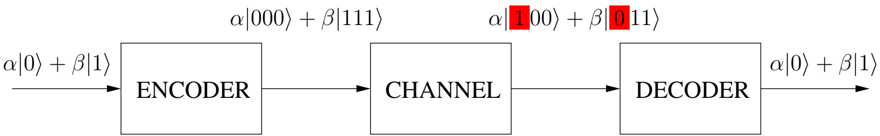
Pauli-to-Classical Isomorphism

Classical Error Correction



Pauli-to-Classical Isomorphism

Quantum Error Correction



$\alpha|0\rangle + \beta|1\rangle$

ENCODER

$\alpha|000\rangle + \beta|111\rangle$

CHANNEL

$\alpha|100\rangle + \beta|011\rangle$

DECODER

$\alpha|0\rangle + \beta|1\rangle$

We wish to determine the error without observing the qubit!!

Solution: Measure the error without reading the data.

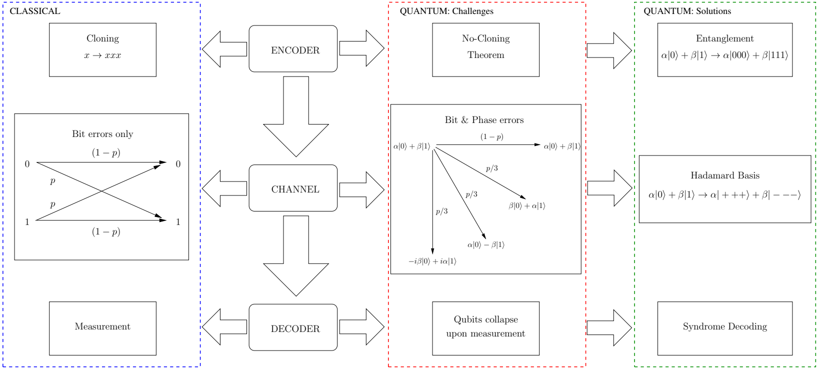
Pauli-to-Classical Isomorphism

Quantum Error Correction → Syndrome Decoding

- Check 1: Modulo 2 addition of first and second qubits.
- Check 2: Modulo 2 addition of first and third qubits.

Syndrome (s)	**Correction**
00	No Error
11	Bit error on 1st Qubit
10	Bit error on 2nd Qubit
01	Bit error on 3rd Qubit

Pauli-to-Classical Isomorphism



CLASSICAL

Cloning
$x \to xxx$

Bit errors only

$(1-p)$
0
0
p
p
1
1
$(1-p)$

Measurement

ENCODER

CHANNEL

DECODER

QUANTUM: Challenges

No-Cloning
Theorem

Bit & Phase errors

$\alpha|0\rangle + \beta|1\rangle$
$(1-p)$
$\alpha|0\rangle + \beta|1\rangle$
$p/3$
$\beta|0\rangle + \alpha|1\rangle$
$p/3$
$\alpha|0\rangle - \beta|1\rangle$
$p/3$
$-i\beta|0\rangle + i\alpha|1\rangle$

Qubits collapse
upon measurement

QUANTUM: Solutions

Entanglement
$\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle$

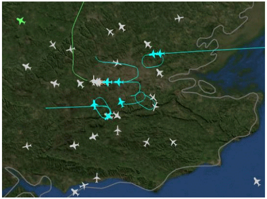
Hadamard Basis
$\alpha|0\rangle + \beta|1\rangle \to \alpha|+{+}+\rangle + \beta|-{-}-\rangle$

Syndrome Decoding

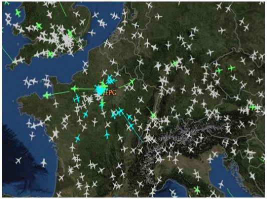
Quantum-Assisted Routing Design Example: Multi-Component Pareto Optimization - BER, DELAY, POWER & COMPLEXITY

- Alanis, D.; Botsinis, P.; Babar, Z.; Ng, S.X.; Hanzo, L.: Non-Dominated Quantum Iterative Routing Optimization for Wireless Multihop Networks, IEEE Access
- Alanis, D. ; Botsinis, P. ; Soon Xin Ng ; Hanzo, L.: Quantum-Assisted Routing Optimization for Self-Organizing Networks: IEEE Access, Volume: 2, 2014, pp 614 - 632

Aircraft mobility pattern for LHR, in the European airspace and over the North Atlantic



Heathrow Airport

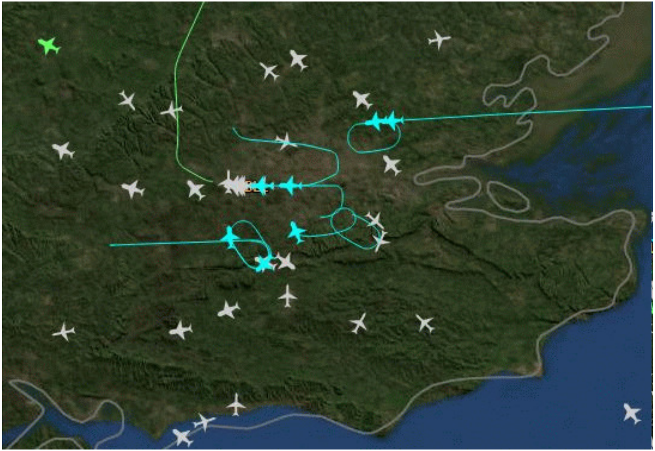


European Airspace

North Atlantic

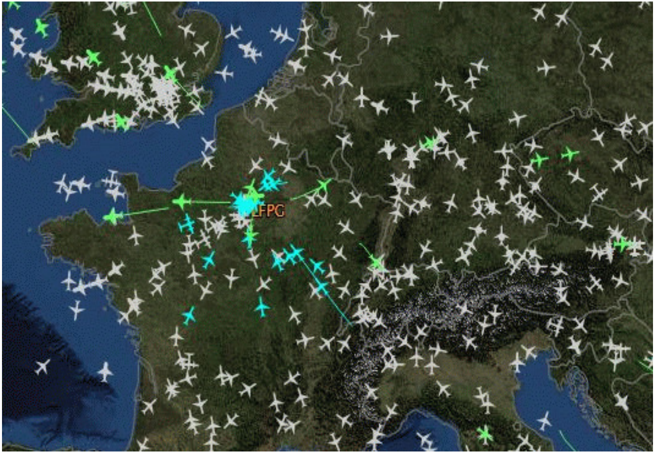
- https://uk.flightaware.com/live/airport/EGLL

Aircraft mobility pattern for London Heathrow airport from flight-aware.



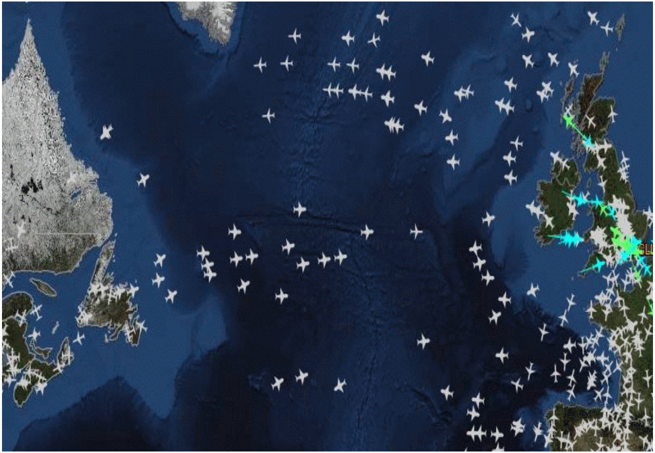
Heathrow Airport

Aircraft mobility pattern for the European airspace from flight-aware.



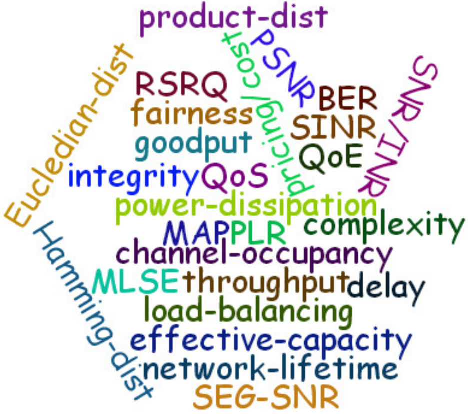
European Airspace

Aircraft mobility pattern in an unpopulated area over the North Atlantic from flight-aware.



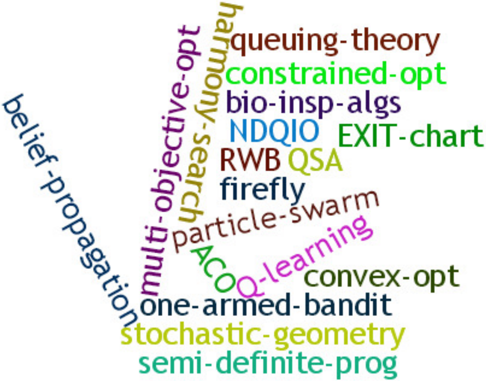
North Atlantic

The Choice of the Objective Function is More influential Than the Optimization Tool...



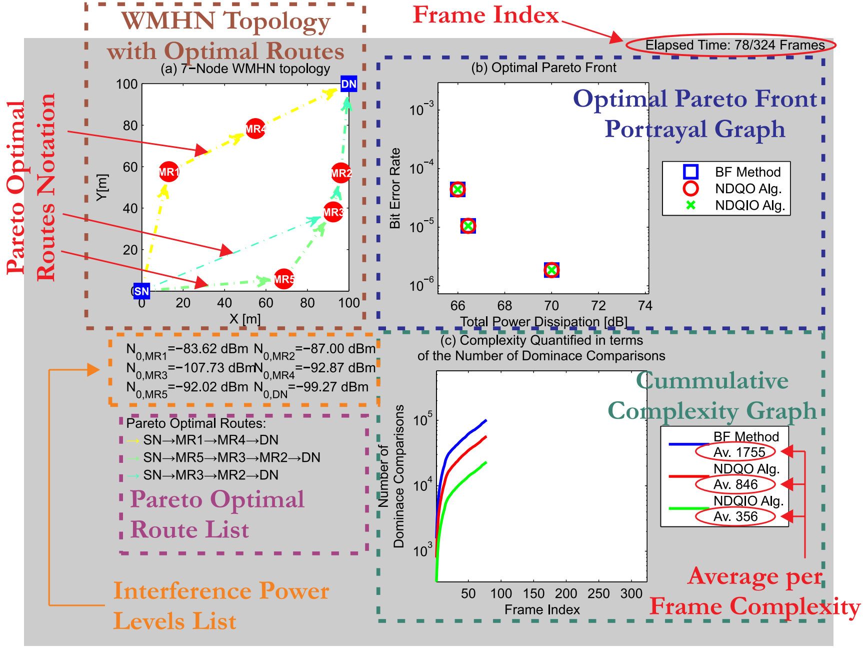
On Course to the Gate of Happiness - Optimization...

Multi-Component Optimization Tools Are Required for Pareto-Optimal Solutions...



Pareto Optimization - The Four Metrics

- Transmit Power;
- BER;
- Delay;
- Complexity, ie. DSP Power-Dissipation;



Elapsed Time: 78/324 Frames

$N_{0,MR1}$=−83.62 dBm $N_{0,MR2}$=−87.00 dBm
$N_{0,MR3}$=−107.73 dBm $N_{0,MR4}$=−92.87 dBm
$N_{0,MR5}$=−92.02 dBm $N_{0,DN}$=−99.27 dBm

Pareto Optimal Routes:
→ SN→MR1→MR4→DN
→ SN→MR5→MR3→MR2→DN
→ SN→MR3→MR2→DN

WMHN Topology with Optimal Routes

Frame Index

Pareto Optimal Routes Notation

Optimal Pareto Front Portrayal Graph

Cummulative Complexity Graph

Pareto Optimal Route List

Interference Power Levels List

Average per Frame Complexity

- P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Physical Review A*, vol. 52, no. 4, 1995.
- A. M. Steane, “Error correcting codes in quantum theory,” *Physical Review Letters*, vol. 77, no. 5, 1996.
- R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, “Perfect quantum error correcting code,” *Physical Review Letters*, vol. 77, no. 1, 1996.
- D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.
- A. Y. Kitaev, “Quantum computations: Algorithms and error correction,” *Russian Mathematical Surveys*, vol. 52, no. 6, pp. 1191–1249, 1997.
- A. Y. Kitaev, “Fault-tolerant quantum computation by anyons,” *Annals of Physics*, vol. 303, no. 1, pp. 2–30, 2003.
- S. B. Bravyi and A. Y. Kitaev, “Quantum codes on a lattice with boundary,” *arXiv preprint quant-ph/9811052*, 1998.
- A. R. Calderbank, E. M. Rains, P. Shor, and N. J. Sloane, “Quantum error correction via codes over GF(4),” *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.
- M. Grassl and T. Beth, “Quantum BCH codes,” in *Proceedings of International Symposium Theoretical Electrical Engineering, 1999*, 1999.
- M. Grassl, W. Geiselmann, and T. Beth, “Quantum Reed-Solomon codes,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pp. 231–244, Springer, 1999.
- A. M. Steane, “Quantum Reed-Muller codes,” *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1701–1703, 1999.
- G. Bowen, “Entanglement required in achieving entanglement-assisted channel capacities,” *Physical Review A*, vol. 66, no. 5, 2002.

T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, 2006.

H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Physical Review Letters*, vol. 91, no. 17, 2003.

M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Physical Review A*, vol. 81, no. 4, 2010.

M. S. Postol, "A proposed quantum low density parity check code," *arXiv preprint quant-ph/0108131*, 2001.

D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, 2004.

T. Camara, H. Ollivier, and J.-P. Tillich, "Constructions and performance of classes of quantum LDPC codes," *arXiv preprint quant-ph/0502086*, 2005.

T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: Construction and performances under iterative decoding," in *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2007*, pp. 811–815, 2007.

M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Physical Review A*, vol. 79, no. 3, 2009.

Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, 2015.

H. Bombin and M. A. Martin-Delgado, "Topological quantum distillation," *Physical Review Letters*, vol. 97, no. 18, 2006.

D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2776–2798, 2009.

M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2011*, pp. 445–449, 2011.

M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1203–1222, 2014.

Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

G. Zémor, "On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction," in *Proceedings of International Conference on Coding and Cryptology, 2009*, pp. 259–273, 2009.

A. Couvreur, N. Delfosse, and G. Zemor, "A construction of quantum LDPC codes from Cayley graphs," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 6087–6098, 2013.

J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," in *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2009*, pp. 799–803, 2009.

A. A. Kovalev and L. P. Pryadko, "Improved quantum hypergraph-product LDPC codes," in *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2012*, pp. 348–352, 2012.

J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1193–1202, 2014.

J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Physical Review Letters*, vol. 109, no. 5, 2012.

M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," in *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2012*, pp. 334–338, 2012.

N. Delfosse, "Tradeoffs for reliable quantum information storage in surface codes and color codes," in *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2013*, pp. 917–921, 2013.

S. Bravyi and M. B. Hastings, "Homological product codes," in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing, 2014*, pp. 273–282, 2014.